UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

DOCUMENT NUMBER: UID _605_ECMP

AADHAAR ENROLMENT CLIENT- PUBLIC KEY INTEGRATION

DOCUMENT VERSION 2.1

ENROLMENT CLIENT APPLICATION VERSION 2.1

Table of Contents

1. Introduction

The document provides the answers for the FAQ on registrar certificate. The document is to make the registrars understand the certificates.

1.1 Certificates FAQ

PKI.2.1 Definition

In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt/decrypt the messages and digital signatures.

The use of combined public and private keys is known as asymmetric cryptography.

PKI.2.2 Process Introduction

The AADHAAR Enrolment Client application captures the demographic and biometric data of the residents. All the data collected by UIDAI will be encrypted with a 1024 / 2048 bit public key. In order for the registrars to get access to the enrolment packets specific to registrars, it is essential for them to provide their public key to the UIDAI. The public key file should be digitally signed by the CA for validation. UIDAI would integrate the given public key with the enrolment client. A release would be made with the available key to the respective registrars.

PKI.2.3 Why should registrars provide rather than UID generating these keys and providing the same.

The data that we deal with are very personal to the residents of this country. It is essential to ensure 100% security of the data. In order to avoid all misuse and handling UIDAI recommends the registrars to create the keys in a secured place and only provide the public key to the CA or ask the CA's to provide the certificate token protected with a pin. UID providing this token would be violation of security policies. CA's run the certificates as business and they have various standards that are built to ensure the keys are from the correct person and avoid all security risks associated with Man in the middle attacks.

PKI.2.4 When should the Registrar provide Public Key?

The public key should be provided as soon as possible during the Registrar On boarding Process. It is recommended that the registrars provide Public Key to UIDAI at least 30 days before the start of enrolments.

PKI.2.5 Is there a format to the Public Key?

The accepted Public Key Format for the AADHAAR enrolment client application is X509 certificate. The public key size would 2048 bits.

PKI.2.6 I am a Registrar and how do I get a Public Key?

The registrar could generate a public/private key pair and get it signed by any of the trusted CA. A class 3/Class 2 level certificate for an organization would be enough to prove the trust. The process is very similar to buying a web server class certificate.

PKI.2.7 What about the private key what should Registrar do with them?

For all the certificates there would be a corresponding private key. The private key is the most sensitive and secret part of the entire activity. It is highly recommended that the Registrars store the private key in encrypted format or use HSM to store the private keys. Private keys should be encrypted with strong passwords at rest and at motion to ensure the safety of the key.

The private keys are used by the registrars to decrypt the packet.

PKI.2.8 How should a Registrar provide Public Key?

The public key can be emailed by the registrar to TechSupport@uidai.gov.in, and a copy can be marked to the UIDAI Nodal Officer and UIDAI PMU coordinator.

PKI.2.9 How do Registrars test their public Key?

When UIDAI releases and send Aadhaar Enrolment Client to the Registrar, the registrars should create enrolment packets, and decrypt the same using the Private Key, corresponding to their Public key. UIDAI also provides a sample utility to decrypt the packet.

Registrars can make a request to UIDAI for sample enrolment packets encrypted with their public key by sending an email to TechSupport@uidai.gov.in.

PKI.2.10 Common Mistakes that registrar do while buying digital certificates.

Registrars are not supposed to buy a digital signature. UIDAI needs digital certificate, with a public key to encrypt the data and not digital signatures.

PKI.2.11 How do i generate a Public/Private key pair?

The tool called open ssl to generate a public private key. The open ssl tool is a free tool available online for download. Ensure to use a proper secure pin to encrypt your private key.

PKI.2.12 What should I do Public/Private key pair?

The private key is supposed to keep in a secured environment. The public has to be given to the CA to certify. The CA will get your public keys and will provide a class 3 X509 DER encoded certificate. Please send this X509 DER encoded certificate to the UIDAI.

PKI.2.13 Where is the utility to decrypt the data?

This test decryptor utility is developed to assist Registrars in decrypting the Registrar Enrolment Packets before go-live. This utility supports only **PFX, PEM, P12 & tokens directly** for private key files. The private key files/Crypto tokens must be password protected. The decryptor tool and the source code is available at http://developer.uidai.gov.in/site/downloads

This is designed purely as a test tool along with source code provided for initial testing. THIS IS NOT SUPPORTED SOFTWARE.